REMARKS

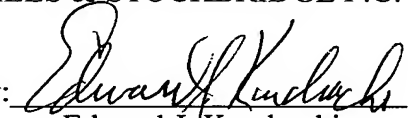
Favorable consideration of the present application is respectfully requested.

This Preliminary Amendment is filed in order to remove the multiple dependencies from the claims. This has been effected by canceling all of existing Claims 1-19 and presenting new Claims 26-39.

Early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

By: 
Edward J. Kondracki
Reg. No. 20,604

1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone: (703) 610-8627
#9220577v1

AMENDED CLAIMS

1. Group signature hardware system enabling a member (M) of a group (G) to produce a message (m) accompanied by a signature (s) proving to a checker (2, 4) that the said message originates from a member of this group (G), using a personalized data (z; Kz),

characterized in that it is electronic and in that the said personalized data is in a form integrated into this electronic hardware support (26).

2. Hardware support according to claim 1, characterized in that it includes encryption means (B3) to make a personalized encrypted text (C) using the said personalized data (z; Kz) before the signature S of the message (m).

3. Hardware support according to claim 2, characterized in that it also includes means (B5) of making a combination of a message (m) to be signed and the encrypted text C associated with this message, in the form of a concatenation of the message m with the encrypted text (C).

4. Hardware support according to any one of claims 1 to 3, characterized in that it also includes means (B6) of signature (Sig) of the message (m) with the personalized data (z; Kz) in encrypted form associated with this message (C).

5. Hardware support according to any one of claims 2 to 4, characterized in that the said personalized data is an

identifier (z) personal to the member (M), and in that the said electronic hardware support (26) also includes an encryption key (K) common to all members of the group (G), and encryption means (B3) to encrypt (C) the identifier with the said encryption key.

6. Hardware support according to claim 5, characterized in that encryption means (B3) encrypt (C) the identifier and a random number (r).

7. Hardware support according to any one of claims 2 to 4, characterized in that the said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G), and in that encryption means (B3) encrypt (C) using at least one data (r) with the said encryption key.

8. Hardware support according to claim 7, characterized in that the said data includes a random number (r).

9. Hardware support according to any one of claims 2 to 8, characterized in that the encryption means (B3) use a secret key encryption algorithm (K), for example the algorithm known as AES (advanced encryption standard).

10. Hardware support according to any one of claims 2 to 8, characterized in that the encryption means (B3) use a public key encryption algorithm, for example the algorithm known as RSA (Rivest, Shamir, Adleman).

11. Hardware support according to any one of claims 4 to 10, characterized in that means (B6) of signature (Sig) use a private key signature algorithm (SK), for example the algorithm known as RSA (Rivest, Shamir, Adleman).

12. Hardware support according to claim 11, characterized in that the signature algorithm is of the RSA type and includes the said PKCS#1 standard as defined particularly in the document "RSA Cryptography Standard - RSA Laboratories - Draft2 - January 5 2001".

13. Hardware support according to any one of claims 1 to 12, characterized in that it is a portable communicating device (26).

14. Hardware support according to claim 13, characterized in that it is a smart card (26).

15. Method for sending a message (m) with a group (G) signature (S) of this message, characterized in that it uses the system according to any one of claims 1 to 14, the signature of the message (m) being produced with a private key (SK) common to members (M) of the group (G) and integrating the personalized data (z; Kz) produced from the electronic hardware support (26), the method providing means of transmitting the message thus signed to a checker (2, 6) without needing to supply proof to the checker that the member (M) belongs to the said group (G), such as a member certificate or proof of possession of such a certificate.

16. Method for checking a message (m) received with a group signature for this message, the message having been sent in accordance with the method according to claim 15, characterized in that the check is made using a public key corresponding to the said private key (SK).

17. Method for opening a signature (S) produced by the system according to any one of claims 1 to 14, characterized in that it comprises steps consisting of:

- making correspondence data between the identities of members (M) of the group (G) and their personalized data available, before the signature;

- decrypting the personalized data received from an electronic hardware support (26) for which the signature is to be opened; and

- making the decrypted personalized data correspond to the identity of the member (M) of the group (G).

18. Method for preparation of an electronic hardware support (26) for the system according to any one of claims 1 to 14, personalized to a member (M) accepted into a group, characterized in that it comprises steps consisting of:

- producing the personalized data (z; Kz) to be used for the said electronic hardware support (26) to be personalized; and

- registering this personalized data with a private signature key (SK) in the said support.

19. Group signature system, including a terminal (10) fitted with means for reading a hardware support (26) according to any one of claims 1 to 14, a server (2), a shopkeeper (6), a trusted authority (4), and a bank (8).